INFORMATION PROCESSOR

Pub. No.: 06-035807 [JP 6035807 A]
Published: February 10, 1994 (19940210)
Inventor: SAKAI TATSUYA
Applicant: SHARP CORP [000504] (A Japanese Company or Corporation), JP (Japan)
Application No.: 04-189329 [JP 92189329]
Filed: July 16, 1992 (19920716)

ABSTRACT
PURPOSE: To provide an information processor which can carry out the security control for each output device.

CONSTITUTION: In regard of the register processing, a user is instructed to select a device for the secret processing (S10). If it is decided that just one of output devices requires the secret processing after confirming whether the secret processing should be applied to the selected output device or not (S11), a key word is requested to the user (S12). Then, the secret processing information and the key word information are registered as a file header part (S13), and this header part is added to such data as the document data, etc., and a data file is registered into an external storage (S14).

(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平6－35807

(43)公開日　平成６年(1994)２月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｃ	9293－5B		

審査請求　未請求　請求項の数２(全　９　頁)

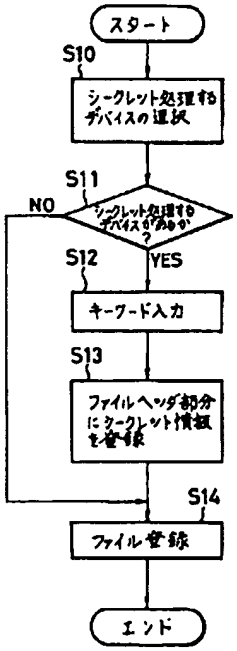
(21)出願番号　特願平4－189329

(22)出願日　平成４年(1992)７月16日

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　酒井　達也
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　弁理士　川口　義雄　(外１名)

(54)【発明の名称】　情報処理装置

(57)【要約】
【目的】　出力デバイス毎にセキュリティ管理を実行できる情報処理装置を提供する。
【構成】　登録時の処理は、表示装置及び入力装置を通じて、利用者に、シークレット処理を行うデバイスを選択させる（ステップＳ１０）。選択された出力デバイスに対してシートクレット処理を実施するかどうかを確認し、出力デバイスどれか１つでもシークレット処理が必要であると指定されたならば（ステップＳ１１）、利用者に対してキーワード要求を行う（ステップＳ１２）。そして、シークレット処理情報及びキーワード情報がファイルヘッダ部分として登録され（ステップＳ１３）、このファイルヘッダ部分を文書データ等のデータに付加してデータファイルが外部記憶装置へ登録される（ステップＳ１４）。



1

【特許請求の範囲】

【請求項1】　記憶装置を有しており、複数の出力デバイスが接続可能な情報処理装置であって、前記記憶装置にデータ又はプログラムファイルを登録する際に、前記出力デバイスの夫々に対して出力可能か否かを示すシークレット情報を前記データ又はプログラムファイルに付加して登録する登録手段と、該登録手段によって登録されたデータ又はプログラムファイルを前記出力デバイスに出力する際に、少なくとも前記データ又はプログラムファイルに付加された該出力デバイスに係わるシークレット情報を基に前記出力デバイスに出力するか否かを判定する判定手段とを備えたことを特徴とする情報処理装置。

【請求項2】　前記登録手段が、キーワード情報をデータ又はプログラムファイルに付加する手段を含んでおり、前記判定手段が、登録された前記データ又はプログラムファイルに付加されたキーワード情報と入力されたキーワード情報とをさらに比較して前記出力デバイスに出力するか否かを判定する手段を含んでいることを特徴とする請求項1に記載の情報処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、シークレット処理機能を有する情報処理装置に関する。

【0002】

【従来の技術】図6及び図7は、従来のワードプロセッサ等の情報処理装置で作成される文書データファイルで使用されているシークレット処理の一例を表す、ファイル登録時及びファイル読込み時のフローチャート図である。

【0003】図6に示すように、文書データをファイル登録する際、登録するファイルをシークレット状態とするかどうかを利用者に確認させ（ステップS40）、シークレット状態とする場合、利用者にキーワードの入力要求をし（ステップS41）、その後、シークレット状態であることを示すデータ及びキーワード（通常は暗号化されている）をファイルのヘッダ部分に登録し（ステップS42）、その後、文書データの登録を実施する（ステップS43）。

【0004】また、図7に示すように、文書データを読み込む際、最初にファイルのヘッダ部分のみを読み込み（ステップS50）、登録されたファイルがシークレット状態であるかを確認し（ステップS51）、シークレット状態である場合、利用者にキーワード入力を要求した（ステップS52）後、そのキーワード入力がファイルのヘッダ部分に登録されているキーワードと一致するかどうか確認を行う（ステップS53）。当然の事ながら入力したキーワードが誤っていれば、エラー表示を行いファイルの読み込みは実施されず（ステップS55）、正しいキーワードであれば、ファイルは読み込まれ（ステップS54）、以後、文書データの編集が可能となる。

2

【0005】この種の処理のために使用される、ディスク全体の内部構造の一例を図8に示す。これは、図6及び図7のフローチャートに従った場合のファイルの内部フォーマットの一例である。

【0006】ディスク全体の情報エリア30は、一般に、ファイルリストエリア31と各ファイルのデータエリア32とを含んでおり、ファイルリストエリア31はファイル名311、ファイルサイズ312、情報エリア30内の格納位置313、及びその他の情報を含むファイルリストテーブルである。各ファイルのデータエリア32は、シークレット状態であるかどうかを表すシークレット情報エリア321とキーワード情報エリア322とを含むヘッダ領域とデータ領域とから構成される。

【0007】

【発明が解決しようとする課題】従来のシークレット処理では、シークレット状態にあるファイルは、キーワードを入力しない限り、一切の使用が認められないものであった。

【0008】この事は、「文書データをプリントアウトされるのは困るが、ディスプレイ上での表示はかまわない」という状況には、対応することができず全く無能な機能であった。

【0009】また、アプリケーションソフトウェアは、一般的にフロッピディスクで提供される。提供されたアプリケーションソフトウェアをコンピュータのハードディスクにインストール処理する場合、ファールのハードディスクへのコピーが実行されるが、フロッピディスクに対するコピープロテクトを実施しながら、ハードディスクへのインストール処理は、従来の情報処理装置では容易なことではなかった。

【0010】また、従来の情報処理装置では、バイナリ形式のファイル（この形式のファイルは、テキスト形式のファイルではないため、このファイル内容を表示、プリンタ出力することは意味がない）もテキスト形式のファイルと同様に管理されていたため、利用者が誤ってバイナリ形式ファイルの表示処理すると、ディスプレイ上に意味のないデータが表示されることもあった。

【0011】従って、本発明は、出力デバイス毎にセキュリティ管理を実行できる情報処理装置を提供するものである。

【0012】

【課題を解決するための手段】本発明によれば、記憶装置を有しており、複数の出力デバイスが接続可能な情報処理装置であって、記憶装置にデータ又はプログラムファイルを登録する際に、出力デバイスの夫々に対して出力可能か否かを示すシークレット情報をデータ又はプログラムファイルに付加して登録する登録手段と、該登録手段によって登録されたデータ又はプログラムファイル

3

を出力デバイスに出力する際に、少なくともデータ又はプログラムファイルに付加された出力デバイスに係わるシークレット情報を基に出力デバイスに出力するか否かを判定する判定手段とを備えた情報処理装置が提供される。

【0013】また、登録手段が、キーワード情報をデータ又はプログラムファイルに付加する手段を含んでおり、判定手段が、登録されたデータ又はプログラムファイルに付加されたキーワード情報と入力されたキーワード情報とをさらに比較して出力デバイスに出力するか否かを判定する手段を含んでいてもよい。

【0014】

【作用】記憶装置にデータ又はプログラムファイルが登録される際に、出力デバイスの夫々に対して出力可能か否かを示すシークレット情報がデータ又はプログラムファイルに付加されて登録される。従って、ある出力デバイスに対しては出力可能であるが、他の出力デバイスに対しては出力不可であるというようなシークレット情報が付加されることになる。

【0015】この様なデータ又はプログラムファイルを出力デバイスに出力する際には、判定手段によってデータ又はプログラムファイル内のシークレット情報が読み取られ、少なくともこの情報を基にその出力デバイスに出力するか否かが判定される。

【0016】

【実施例】以下、本発明に係わる情報処理装置の実施例について図面を用いて説明する。

【0017】図5は、本発明に係わる情報処理装置の一実施例であるパーソナルコンピュータやワードプロセッサなどのシステム構成を表すブロック図である。

【0018】中央処理装置10には、入力装置11、表示装置12、ROM記憶部13、RAM記憶部14、外部記憶装置15、及び各種の出力デバイス16が、バス等を介して接続されている。

【0019】出力デバイス16としては、FDD（フロッピディスクドライブ）、HDD（ハードディスクドライブ）、プリンタ、及びディスプレイが設けられている。

【0020】文書データ等のデータをファイルとして登録する機能を有するファイルシステムコード部13aは、ROM記憶部13に存在する。通常、多くの情報処理装置では、ファイルシステムコード部は外部記憶装置内に存在しており、電源ON時に外部記憶装置からRAM記憶部へと展開されているが、以下の説明を簡単にするため、ここでは、ROM記憶部に存在するものとする。

【0021】ファイルの登録処理とは、ファイルシステムコード部13aが、RAM記憶部14に存在するデータ（例えば文書データ）を、中央処理装置10を通じて外部記憶装置15に登録することを表し、また、その逆に、ファイルの読み込み処理とは外部記憶装置15に存在するデータをファイルシステムコード部13aが、中央処理装置10を通じてRAM記憶部14に読み込みことを表す。尚、ファイル登録の際には、ファイル名やシークレット情報などの管理情報も登録している。外部記憶装置の内部構造については後述する。

4

【0022】図1から図3に、本実施例による情報処理装置におけるシークレット処理のフローチャート図を示す。

【0023】図1は、ファイル登録時のフローチャート図であり、図2は、ファイル読み込み時のフローチャート図であり、図3は、ファイル出力時のフローチャート図である。

【0024】図1に示すように、登録時の処理は、表示装置及び入力装置を通じて、利用者に、シークレット処理を行うデバイスを選択させる（ステップS10）。選択された出力デバイスに対してシートクレット処理を実施するかどうかを確認し、出力デバイスどれか1つでもシークレット処理が必要であると指定されたならば（ステップS11）、利用者に対してキーワード要求を行う（ステップS12）。そして、シークレット処理情報及びキーワード情報がファイルヘッダ部分として登録され（ステップS13）、このファイルヘッダ部分を文書データ等のデータに付加してデータファイルが外部記憶装置へ登録される（ステップS14）。

【0025】尚、記憶装置にデータ又はプログラムファイルを登録する際に、出力デバイスの夫々に対して出力可能か否かを示すシークレット情報をデータ又はプログラムファイルに付加して登録する登録手段は、ステップS10からステップS14に対応している。

【0026】図4は、本実施例による情報処理装置の外部記憶装置、即ちディスク全体の内部構造の一例を示しているメモリマップ図であり、図1のフローチャートに従った場合のファイルの内部フォーマットを示している。

【0027】外部記憶装置、即ちディスクの物理情報エリア20は、一般に、ファイルリストエリア21と各ファイルのデータエリア22とを含んでおり、ファイルリストエリア21はファイル名211、ファイルサイズ212、物理情報エリア20内の格納位置213、及びその他の情報を含むファイルリストテーブルである。各ファイルのデータエリア22は、各出力デバイスに対するシークレット状態を示す情報（例えば、シークレットなしは0、シークレット状態は1）を含むシークレット情報エリア221とパスワード情報エリア222を含むヘッダ領域とデータ領域223とから構成される。

【0028】読み込み時の処理は、図2に示すように、外部記憶装置内に格納されているデータを、単にシートクレット処理情報及びキーワード情報が存在するファイルヘッダを含んで、ファイルをRAM記憶部上に展開す

5

るのみである（ステップＳ２０）。従来と大きく事なる点は、読み込み処理時には、シークレット処理は行わない点である。

【００２９】シークレット処理は、ＲＡＭ記憶部上に読み込まれたファイルを取り扱う際に実施される。

【００３０】図３に示すように、あるデバイスに対してファイル内容の出力要求が発生した場合、このファイルは出力すべきデバイスに対して、シークレット状態となっているかを、ＲＡＭ記憶部上に読み込まれたシークレット情報をもとに判定し（ステップＳ３０）、シークレット状態であれば、キーワード入力を利用者に要求する（ステップＳ３１）。次に、入力されたキーワードとＲＡＭ記憶部上に展開されているキーワード情報とが一致するか否かを判定する（ステップＳ３２）。当然のことながら、キーワードが一致しなければ、ファイル内容の出力は実施されずにエラーとなる（ステップＳ３４）。キーワードが一致すればファイル内容の対応する出力デバイスへの出力処理が実施される（ステップＳ３３）。

【００３１】尚、図１に示した登録手段によって登録されたデータ又はプログラムファイルを出力デバイスに出力する際に、少なくともデータ又はプログラムファイル内の出力デバイスに係わるシークレット情報を基に出力デバイスに出力するか否かを判定する判定手段は、ステップＳ３０からステップＳ３２に対応している。

【００３２】従って、上記実施例によれば、各種出力デバイス（ディスプレイ、プリンタ、フロッピディスク、ハードディスクなど）毎に、シークレット処理を実施するかどうかのシークレット情報を有しているので、ファイルのシークレット状態にもデバイスに対応したレベル付けが可能となる。

【００３３】即ち、本実施例を用いた情報処理装置では、「キーワードの入力なしで、ディスプレイへの表示は可能だが、プリンタへの出力は、キーワードの入力が必要である」という処理が容易に実現でき、より利用者の使用状況にあったシステム提供が可能となる。ディスプレイへの表示が可能で、プリンタへの出力が不可能といった状況を利用者が求める理由は、ディスプレイへの表示は、そのファイル（ディスク）フォーマットにあったシステム（ワードプロセッサなら各機種毎にファイルシステムが異なったり、他社のワードプロセッサは同一フォーマットでないなどから）が必要であるゐ、簡単なプロテクトがかかっていることになるが、一度でもプリントアウトされると、コピーされる危険性が非常に高まるためである。

【００３４】また、本実施例を利用した情報処理装置では、利用者レベルでの簡単なコピープロテクトも実現できる。これは、フロッピディスクに対してシークレット属性を与えることである。情報処理装置は、ファイルコピーを実施する際に、そのファイルのシークレット状態を確認し、もし、フロッピディスクに対してシークレット属性が確認された場合、キーワード入力を要求することになる。

6

【００３５】その他に、ハードディスクへのインストール処理（アプリケーションソフト構築処理）にも有効なものとなる。通常、アプリケーションソフトウェアは、フロッピディスクで提供される。本実施例では、フロッピディスクに対するシークレット処理とハードディスクに対するシークレット処理は別々に管理されるため、フロッピディスクに対するコピープロテクトを実施しながら、ハードディスクへのインストール処理（インストール処理を実施するには、通常、ファイルのコピー処理が必要となる）が可能となる。

【００３６】また、従来の情報処理装置では、バイナリ形式のファイル（この形式のファイルは、テキスト形式のファイルではないため、このファイル内容を表示、プリンタ出力することは意味がない）もテキスト形式のファイルと同様の管理されていたため、利用者が誤ってバイナリ形式ファイルの表示処理すると、ディスプレイ上に意味のないデータが表示されたが、本実施例による情報処理装置では、バイナリ形式のファイルをディスプレイ及びプリンタに対して、シークレット属性を与えることで、この問題も解決できる。

【００３７】

【発明の効果】以上詳細に説明したように、本発明による情報処理装置は、記憶装置を有しており、複数の出力デバイスが接続可能な情報処理装置であって、記憶装置にデータ又はプログラムファイルを登録する際に、出力デバイスの夫々に対して出力可能か否かを示すシークレット情報をデータ又はプログラムファイルに付加して登録する登録手段と、該登録手段によって登録されたデータ又はプログラムファイルを出力デバイスに出力する際に、少なくともデータ又はプログラムファイルに付加された出力デバイスに係わるシークレット情報を基に出力デバイスに出力するか否かを判定する判定手段とを備えたので、各種出力デバイス（ディスプレイ、プリンタ、フロッピディスク、ハードディスクなど）毎に、シークレット処理を実施するかどうかの情報を有している。これによって、ファイルのシークレット状態にも出力デバイス毎にレベル付をすることが可能となり、出力デバイス毎にデータ又はプログラムファイルのセキュリティ管理を実行できる。

【図面の簡単な説明】

【図１】本発明に係わる情報処理装置におけるファイル登録処理を示すフローチャート図である。

【図２】本発明に係わる情報処理装置におけるファイル読み取り処理を示すフローチャート図である。

【図３】本発明に係わる情報処理装置におけるファイル出力処理を示すフローチャート図である。

【図４】本発明に係わる情報処理装置の一実施例の外部記憶装置のメモリマップ図である。

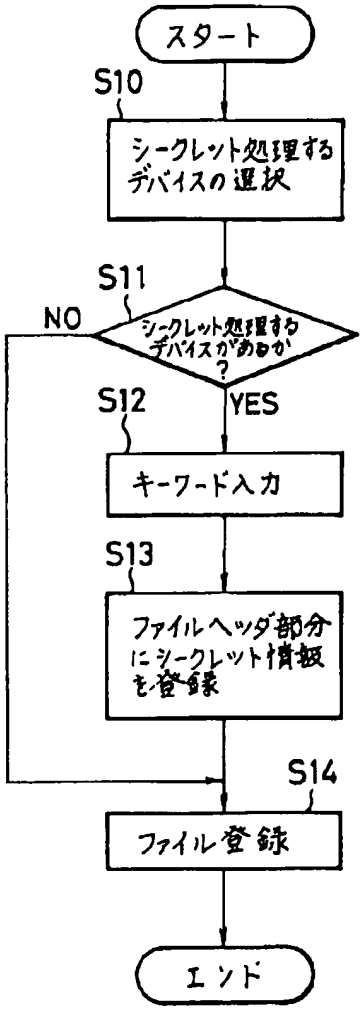
7

【図5】本発明に係わる情報処理装置の一実施例のシステム構成を示すブロック図である。
【図6】従来の情報処理装置におけるファイル登録処理を示すフローチャート図である。
【図7】従来の情報処理装置におけるファイル読み取り処理を示すフローチャート図である。
【図8】従来の情報処理装置の外部記憶装置のメモリマップ図である。

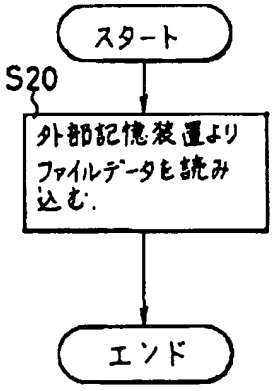
8

【符号の説明】
10　中央処理装置
11　入力装置
12　表示装置
13　ROM記憶部
14　RAM記憶部
15　外部記憶装置
16　出力デバイス

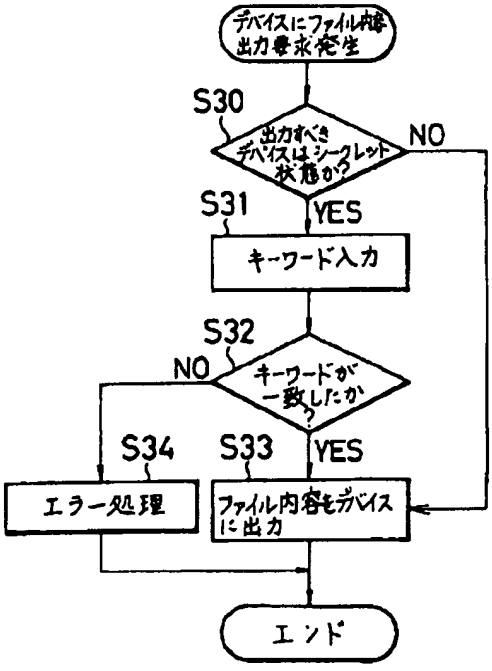
【図1】



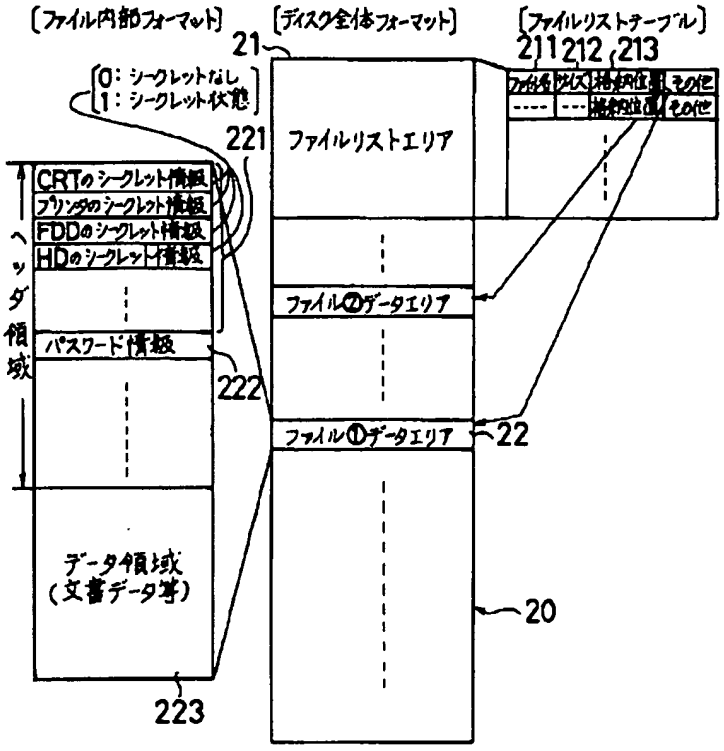
【図2】



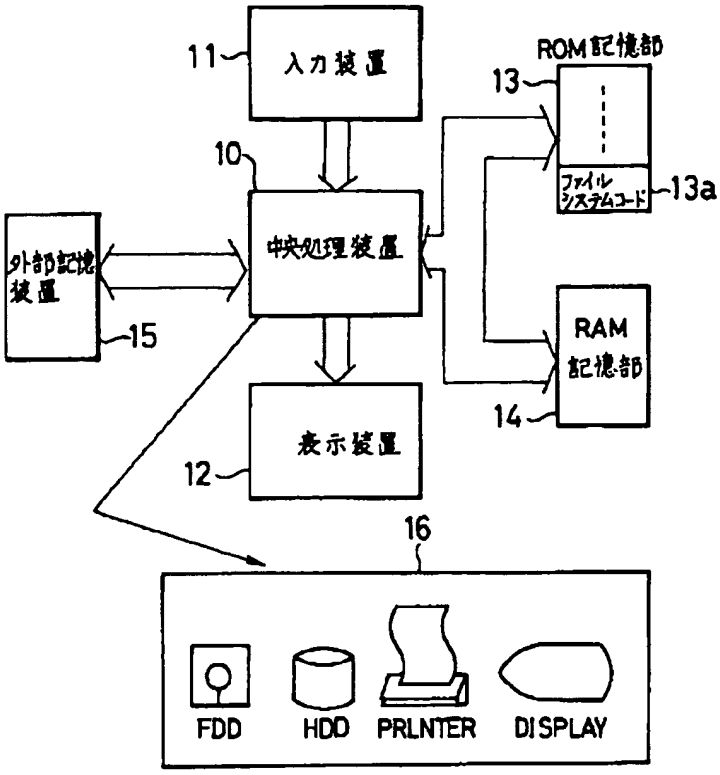
【図3】



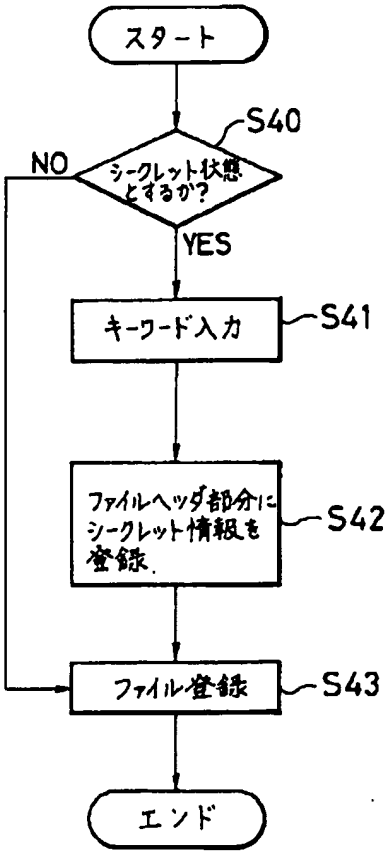
【図4】


〔ファイル内部フォーマット〕
〔ディスク全体フォーマット〕
〔ファイルリストテーブル〕
21
211 212 213
0：シークレットなし
1：シークレット状態
221
ファイルリストエリア
CRTのシークレット情報
プリンタのシークレット情報
FDDのシークレット情報
HDのシークレット情報
ヘッダ領域
パスワード情報
222
ファイル②データエリア
ファイル①データエリア
22
データ領域
（文書データ等）
20
223

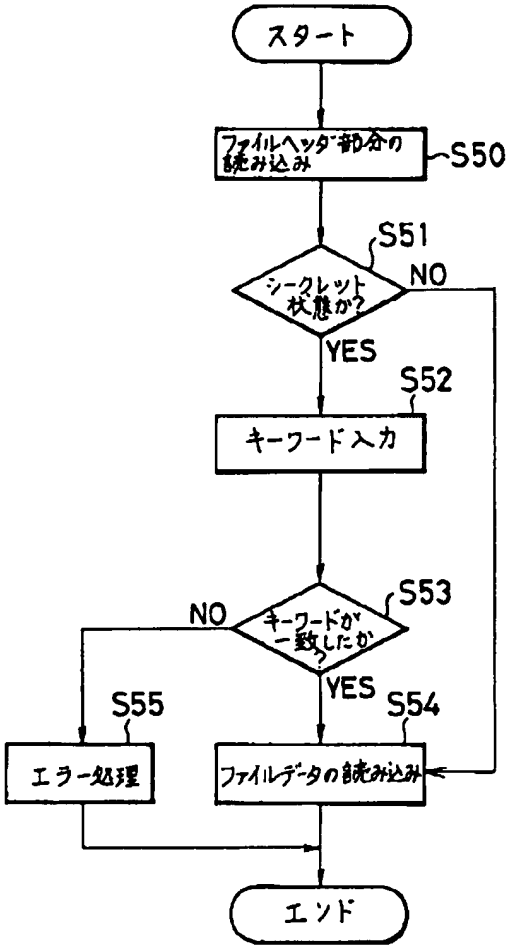
【図5】


11
入力装置
ROM記憶部
13
ファイルシステムコード
13a
10
中央処理装置
外部記憶装置
15
RAM記憶部
14
表示装置
12
16
FDD
HDD
PRLNTER
DISPLAY

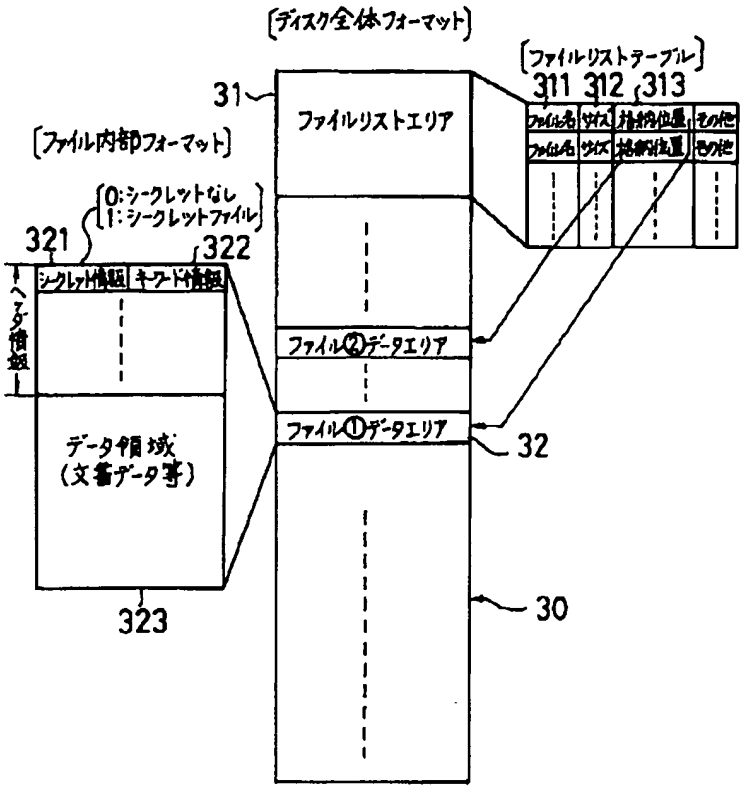
【図6】


スタート
S40
NO
シークレット状態とするか?
YES
キーワード入力
S41
ファイルヘッダ部分にシークレット情報を登録
S42
ファイル登録
S43
エンド

【図7】


スタート
ファイルヘッダ部分の読み込み
S50
S51
シークレット状態か?
NO
YES
S52
キーワード入力
S53
NO
キーワードが一致したか?
YES
S55
S54
エラー処理
ファイルデータの読み込み
エンド

【図8】


〔ディスク全体フォーマット〕
〔ファイルリストテーブル〕
311
312
313
31
ファイルリストエリア
〔ファイル内部フォーマット〕
0:シークレットなし
1:シークレットファイル
321
322
シークレット情報
キーワード情報
ヘッダ情報
ファイル②データエリア
ファイル①データエリア
データ領域
(文書データ等)
32
323
30